UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/059,182	01/31/2002	Janne Suuronen	004770.00521	5357

72165 7590 12/17/2010
BANNER & WITCOFF, LTD
ATTORNEYS FOR CLIENT 004770
1100 13TH STREET
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
SHAW, YIN CHEN	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
12/17/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/059,182
Filing Date: January 31, 2002
Appellant(s): SUURONEN ET AL.

Mark E. Wilinski
(Reg. No. 63,230)

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed Oct. 04, 2010 appealing from the Office action mailed May 11, 2010.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments

The appellant's statement of the status of amendments contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Claims Appendix to the brief is correct.

(8) Evidence Relied Upon

Fink et al. (U.S. Patent 6,496,935 B1; Date of Patent: Dec. 17, 2002);

Joyce (U.S. Patent 6,519,703 B1; Date of Patent: Feb. 11, 2003);

Baum et al. (U.S. Patent 6,400,707 B1; Date of Patent: Jun. 04, 2002);

Lyle (U.S. Patent 6,886,102 B1; Date of Patent: Apr. 26, 2005).

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 4-5, 11, 32-34, 40-50, 53, 56-63, and 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935) and further

in view of Joyce (U.S. Patent 6,519,703) and Baum et al. (U.S. Patent 6,400,707).

i. *Referring to Claims 1, 49, 50, and 62:*

As per Claim 1, Fink et al. disclose an apparatus comprising:

a firewall **[(fig. 1)]** configured to:

receive data packets over a first network **[Packets which are permitted to pass through gateway 15 from external network 14 are then received by one of a plurality of protected nodes 20 (lines 335-37, Col. 5)]**;

classify the received data packets based on the contents of the data packets into packets of a first type and second type **[inspects the contents of such packet or packets (line 67, Col. 6). Pre-filtering module 30 also preferably features a classification engine 38, including a data processor, for at least partially analyzing the information from the packet (lines 4-6, Col. 8)]**;

Fink et al. do not expressly disclose the remaining limitations of the claim. However, Joyce discloses packets which cannot contain virus and packets which can contain a virus and the virus scanning engine for testing if the packet contains virus **[Prior to use, heuristic firewall 10B is trained to perform specific desired tasks. In this embodiment, for example, a first heuristic stage 36 is trained to recognize absolute high-confidence traffic, computer virus and Trojan**

signatures, denial-of-service attack signatures, and other computer security exploit signatures. After training and during use, if heuristic stage 36 clears a packet stream with a "high-confidence" rating (i.e., an analysis of the packets 22 by heuristic stage 36 results in a high level of confidence that the packet stream does not contain threats that heuristic stage 36 is trained to detect), buffer 24 releases the packets into a secured channel 38 directly into network 30. If heuristic stage 36 processing results in only a lesser confidence rating (i.e., a "good-confidence" rating) that threats are absent, buffer 24 releases the packets into a traditional firewall rule base 12 for standard processing. In this case, the output of traditional firewall rule base 12 is buffer 28. If heuristic stage 36 determines that the packet stream is certainly corrupted or otherwise undesired or that threats are detected ("poor-confidence"), buffer 24 shunts the packets elsewhere, for example, either out of the firewall (e.g., to a "bit bucket" such as /dev/null, where they are discarded) or it shunts them elsewhere 26 for additional processing. If heuristic stage 36 is not certain as to the validity of the packets ("marginal-confidence"), buffer 24 releases the packets into complex firewall rule base 14 for processing. The output of complex firewall rule base 24 is buffer 40 (lines 32-58, Col. 3)]; and forward the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine **[rating (i.e., an analysis of the packets 22 by heuristic stage 36 results in a high level of confidence that the packet stream does not contain threats that heuristic stage 36 is trained to detect), buffer 24 releases the packets into a secured channel 38 directly into network 30 (lines 30-43, Col. 3)]** and forward the data packets of the second type of a virus scanning engine for testing **[buffer 24 shunts the packets elsewhere, for example, either out of the firewall (e.g., to a "bit bucket" such as /dev/null, where they are discarded) or it shunts them elsewhere 26 for additional processing. If heuristic stage 36 is not certain as to the validity of the packets ("marginal-confidence"), buffer 24 releases the packets into complex firewall rule base 14 for processing (lines 51-57, Col. 3). If heuristic stage 36 rates packets 22 as either good-confidence or marginal-confidence, the packets are forwarded to another heuristic stage 44. Heuristic stage 44 is pre-trained to look for temporal and other anomalies in packet streams including, but not limited to, one or more of the following: temporal attack signatures, frequency analysis, in-transit packet modification, forged-packet indicators, out-of-band (OOB) communications, and/or covert channel communications (lines 59-67, Col. 39)]**.

Fink et al. and Joyce are analogous art because they are from similar technology relating to information security and packet scanning. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine the system disclosed in Fink et al. with Joyce since one would have been motivated to provide methods and apparatus for a heuristic firewall that can learn from and adapt to data flowing through them to better mitigate such security threats (lines 34-37, Col. 1 from Joyce).

Fink and Joyce do not expressly disclose the remaining limitation of the claim. However, Baum et al. disclose the limitation regarding classifying the received data packet includes determining whether at least one of the data packets includes content for a real-time audio or video data stream by teaching analyzing the packet is of voice (real-time) data **[(lines 41-59, Col. 2; lines 61-62, Col. 5; and lines 25-57, Col. 6; lines 20-22, Col. 7 from Baum)]**;

Fink et al., Joyce, and Baum et al. are analogous art because they are from similar technology relating to information security and packet scanning. It would have been obvious to one of ordinary skill in the art at the time of invention was made to combine the system disclosed in Fink et al. and Joyce with Baum et al. since one would have been motivated to provide methods and apparatus for a firewall that filter the content of the real-time stream in order to provide real time firewall security (lines 11-13, Col. 1 Baum et al.).

As per Claim 49, it is a method claim that corresponds to the apparatus claim 1. Therefore, Claim 49 is rejected for the same rationale as of Claim 1.

As per Claim 50, it is storage medium claim that corresponds to the apparatus claim 1. In addition, Fink et al. disclose a computer program stored on a storage medium **[The device comprising: (a) a memory for storing at least on instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)]**. Therefore, Claim 50 is rejected for the same rationale as of Claim 1.

As per Claim 62, it is an apparatus claim that shares similar limitations as of claim 1. In addition, Fink et al. disclose memory and processor **[The device comprising: (a) a memory for storing at least on instruction (lines 22-23, Col. 3). The method of the present invention could be described as a series of steps performed by a**

data processor, and as such could optionally be implemented as software, hardware, firmware, or a combination thereof (lines 63-66, Col. 3)]. Therefore, Claim 62 is rejected for the same rationale as of Claim 1.

ii. *Referring to Claims 4 and 58:*

As per Claim 4, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1 comprising:

wherein the classifying comprises determining that data packets of the first type contain real time data **[(lines 1-5, Abstract and lines 32-39, Col. 3 from Joyce)]**. In addition, Baum et al. disclose the limitation regarding the real time data other than the audio or video data stream **[(lines 55-59, Col. 2 from Baum et al.); *where the real data is voice data stream*]**.

As per Claim 58, the rejection of claim 49 is incorporated. In addition, Claim 58 encompasses limitations that are similar to those of Claim 4. Therefore, it is rejected with the same rationale as of Claim 4.

iii. *Referring to Claims 5, 57, 59, and 63:*

As per Claim 5, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 4. Fink et al. and Joyce further disclose wherein the classifying comprises determining that data packets of the first type as in Claim 1, and Baum further discloses classifying (I.e., filtering) the packets which are part of the audio or video data stream **[(lines 41-59, Col. 2; lines 61-62, Col. 5; and lines 25-57, Col. 6 from Baum)]**.

As per Claim 57, the rejection of claim 53 is incorporated. In addition, Claim 57 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 59, the rejection of claim 58 is incorporated. In addition, Claim 59 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

As per Claim 63, the rejection of claim 62 is incorporated. In addition, Claim 63 encompasses limitations that are similar to those of Claim 5. Therefore, it is rejected with the same rationale as of Claim 5.

iv. *Referring to Claim 11:*

As per Claim 11, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, further comprising a buffer configured to store the data packets of the second type while the virus scanning engine is testing the data packets to detect a virus **[(lines 39-65, Col. 2 from Joyce)]**.

v. *Referring to Claims 32, 56, and 60:*

As per Claim 32, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, wherein the firewall is configured to receive from a packet classification database, information defining the first and second types of data packets **[(lines 4-7 and lines 38-41, Col. 8 from Fink et al.)]**.

As per Claim 56, the rejection of claim 50 is incorporated. In addition, Claim 56 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale as of Claim 32.

As per Claim 60, the rejection of claim 49 is incorporated. In addition, Claim 60 encompasses limitations that are similar to those of Claim 32. Therefore, it is rejected with the same rationale as of Claim 32.

vi. Referring to Claim 33:

As per Claim 33, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 32, further comprising:

a virus scanning engine configured to receive from a virus detection database, programming information controlling the testing of the data packets of the second type by the virus scanning engine **[(lines 30-40, Col. 2 from Joyce)]**.

vii. Referring to Claim 34:

As per Claim 34, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, further comprising:

a virus scanning engine configured to receive from a virus detection database, programming information controlling the testing of the data packets of the second type by the virus scanning engine **[(lines 30-40, Col. 2 from Joyce)]**.

viii. *__Referring to Claim 40:__*

As per Claim 40, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, further comprising configured to alert the destination upon detection of a virus in the data packets **[(lines 61-67, Col. 4 from Joyce)]**.

ix. *__Referring to Claim 41:__*

As per Claim 41, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1 wherein the destination is a local area network **[protected network 12 (Fig. 1 from Fink et al.)]**.

x. *__Referring to Claim 42:__*

As per Claim 42, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1 wherein the destination is a personal computer **[protected node 20 (Fig. 1 from Joyce)]**.

xi. *__Referring to Claim 43:__*

As per Claim 43, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, wherein the destination is a second network **[protected network 12 (Fig. 1 from Fink et al.)]**.

xii. *Referring to Claim 44:*

As per Claim 44, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, wherein the first network is a wide area network **[external network 14 (Fig 1 from Fink et al.)]**.

xiii. *Referring to Claim 45:*

As per Claim 45, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 44, wherein the wide area network is the Internet **[External network 14 could optionally be the Internet, for example (lines 28-29, Col. 5 from Fink et al.)]**.

xiv. *Referring to Claim 46:*

As per Claim 46, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, wherein the destination comprises an Internet service provider configured to connect coupled to a gateway,

a modem configured to connect to the Internet service provider, and one of a local area or personal computer configured to connect to the modem **[(Fig. 1 from Fink et al.) and (lines 50-55, Col. 4 from Joyce)]**.

xv. *Referring to Claim 47:*

As per Claim 47, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1, further comprising a virus scanning engine configured to decode the data packets during the testing of the data packets **[(lines 69-67, Col. 3 from Joyce) and (lines 4-11, Col. 7 from Fink et al.)]**.

xvi. <u>*Referring to Claim 48:*</u>

As per Claim 48, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 47, wherein the virus scanning engine is configured to function functions as a proxy for a destination processor configured to receive which receives the data packets **[(Fig. 1 from Fink et al.) and (lines 50-55, Col. 4 from Joyce)]**.

xvii. <u>*Referring to Claim 53:*</u>

As per Claim 53, Fink et al., Joyce, and Baum et al. disclose the method of claim 49. In addition, Baum et al. disclose wherein the classifying comprises that the data packets of the first type include the content for the real-time audio or video data stream **[(lines 41-59, Col. 2; lines 61-62, Col. 5; and lines 25-57, Col. 6 from Baum et al.)]**.

xviii. <u>*Referring to Claim 61:*</u>

As per Claim 61, Fink et al., Joyce, and Baum et al. disclose the method of claim 49, wherein the classifying is performed by a firewall **[(lines 6-8, Col. 5; lines 65-67, Col. 6; lines 4-7, Col. 8 from Fink et al.)]**.

xix. <u>*Referring to Claim 65:*</u>

As per Claim 65, Fink et al., Joyce, and Baum et al. disclose a computer program in accordance with claim 49, wherein the classification is performed by a firewall **[(lines 30-40, Col. 2 and lines 32-58, Col. 3 from Joyce)]**.

2. Claims 6 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fink et al. (U.S. Patent 6,496,935), Joyce (U.S. Patent 6,519,703), and Baum et al. (U.S. Patent 6,400,707) and further in view of Lyle (U.S. Patent 6,886,102).

   i. *Referring to Claims 6 and 54:*

   As per Claim 6, Fink et al., Joyce, and Baum et al. disclose the apparatus of claim 1. Fink et al., Joyce, and Baum et al. disclose the firewall as in Claim 1. Fink et al., Joyce, and Baum et al. do not expressly disclose the remaining limitations of the claim. However, Lyle discloses stop reception of a data stream containing the data packets in response to an alert from the virus scanning engine **[(lines 28-34, Col. 14 from Lyle)]**.

   Fink et al., Joyce, Baum et al., and Lyle are analogous art because they are from similar technology relating to Internet security regarding to data communications. It would have been obvious to one of ordinary skill in the art at the time of invention was made to modify Fink et al., Joyce, and Baum et al. with Lyle to have the various components in the gateway communicating with an alert message if the malicious code is detected, and to stop the data flow into the protected network in such a scenario since one would be motivated to have a way to share information about an attack, dynamically and without human intervention (lines 20-22, Col. 2 from Lyle).

As per Claim 54, the rejection of claim 50 is incorporated. In addition, Claim 54 encompasses limitations that are similar to those of Claim 6. Therefore, it is rejected with the same rationale as of Claim 6.

(10) Response to Argument

Appellants' arguments found on pages 6-9 of the appeal brief, filed on Oct. 04, 2010, with respect to claim rejections under 35 U.S.C. 103(a) for claims 1, 4-6, 11, 32-34, 40-50, 53-54, 56-63, and 65 have been fully considered, but they are not persuasive.

A. <u>Rejection of Claims 1, 4-5, 11, 32-34, 40-50, 53, 56-63, and 65 under 35 U.S.C. § 103(a) over Fink, in view of Joyce and Baum</u>

1. <u>Independent claim 1 and dependent claims 4-5, 11, 32-34, and 41-48</u>

   Examiner respectfully traverses Appellants' assertion that the recited features, "a firewall configured to ... classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, *wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream*", are distinguishable from the applied documents. The prior art by Joyce specifically discloses the recited firewall feature by teaching a firewall system having various heuristic states (see Col. 3, lines 29-67 and Fig. 2). Joyce further discloses the firewall system is to perform the recited classifying step on the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and a packets of a second type which can contain a virus according to the description in Col. 3, lines 32-58. That is, Joyce's step of classifying the received data packets into packets of a first type which cannot contain a virus and a packets of a second type which can contain a virus is to recognize, after analysis, whether a packet stream is of a high-confidence rating such that the packet stream does not contain threats/virus or of other rating(s) such that the packet stream can contain threats/virus. Therefore, contrary to Appellants' assertion, the prior art by Joyce discloses the recited feature regarding "a firewall configured to ... classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and a packets of a second type which can contain a virus".

While the prior art by Joyce teaches the step of classifying the packet stream in the firewall system, it does not expressly disclose the content type of the packet stream. The prior art by Baum, on the other hand, further addresses this deficiency by teaching that the internet communication packet is of either audio or video type. This is evident from the disclosure in Baum in which the disclosed firewall is to perform packetized voice filtering (see Col. 2, lines 41-59). Thus, the combination of Joyce and Baum, at least, addresses the argued feature, "a firewall configured to ... classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and a packets of a second type which can contain a virus, *wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream*", recited in the independent claim 1, and the cited documents/references, as a whole, renders the claim obvious.

Examiner further respectfully traverses Appellants' assertion that claims 4, 5, 11, 32-34, and 41-48, which depend from claim 1, are distinguishable from the applied documents by Fink, Joyce, and Baum for at least the same rationale as stated for the independent claim 1 above. In addition, each of the features of the dependent claims 4, 5, 11, 32-34, and 41-48 is rendered obvious based on the combination of the applied documents by Fink, Joyce, and Baum.

2. Dependent claim 40

Examiner respectfully traverses Appellants' assertion that it is distinguishable from the applied documents as Joyce fails to describe alerting network upon detection of a virus in data packets. It should be noted the rejection of claim 40 depends on the combination of applied prior art by Fink, Joyce, and Baum, and the prior art by Joyce specifically discloses that the claimed destination is the Internet in Col. 4, lines 29-30. Joyce further discloses that in case heuristic stages discover problems, such as existence of virus described in Col. 3, lines 64-67 and Col. 4, lines 40-43, in session data or session data flow, a external call or alternate process such as alarms are provided. The provided alarms, in this case, would be alerting/ pager device providing messages to be transmitted to administrator, security officer, etc... according to description in Col. 4, lines 61-67. That is, the transmission of the alert message would be required to pass through a communication network, such as Internet. Therefore, the disclosure from Joyce has rendered the claim feature regarding "alert the destination upon detection of a virus in the data packets" by teaching the internet network as the destination would have an alert message sent to upon detecting of problems like Trojan or attack signatures in the data flow.

3. Independent claim 49 and dependent claims 58-61

Examiner respectfully traverses Appellants' assertion that the recited features, "classify the data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and packets of a second type that can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream", are distinguishable from the applied documents based on the rationale substantially similar to the one stated for the independent claim 1.

Examiner further respectfully traverses Appellants' assertion that claims 58-61, which depend from claim 49, are distinguishable from the applied documents by Fink, Joyce, and Baum for at least the same rationale as stated for the independent claim 49 above. In addition, each of the features of the dependent claims 58-61 is rendered obvious based on the combination of the applied documents by Fink, Joyce, and Baum.

4. Independent claim 50 and dependent claims 53, 56-57, and 65

Examiner respectfully traverses Appellants' assertion that the recited features, "classify the received data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and packets of a second type that can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream", are distinguishable from the applied documents based on the rationale substantially similar to the one stated for the independent claim 1.

Examiner further respectfully traverses Appellants' assertion that claims 53, 56-57, and 65, which depend from claim 50, are distinguishable from the applied documents by Fink, Joyce, and Baum for at least the same rationale as stated for the independent claim 50 above. In addition, each of the features of the dependent claims 53, 56-57, and 65 is rendered obvious based on the combination of the applied documents by Fink, Joyce, and Baum.

5. Independent claim 62 and dependent claim 63

Examiner respectfully traverses Appellants' assertion that the recited features, "classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream", are distinguishable from the applied documents based on the rationale substantially similar to the one stated for the independent claim 1.

Examiner further respectfully traverses Appellants' assertion that claim 63, which depend from claim 62, are distinguishable from the applied documents by Fink, Joyce, and Baum for at least the same rationale as stated for the independent claim 50 above. In addition, the feature of the dependent claims 63 is rendered obvious based on the combination of the applied documents by Fink, Joyce, and Baum.

B. <u>Rejection of Claims 6 and 54 under 35 U.S.C. § 103(a) over Fink, Joyce, and Baum, and further in view of Lyle</u>

1. <u>Dependent claims 6 and 54</u>

Examiner respectfully traverses Appellants' assertion that dependent claims 6 and 54 are distinguishable for from the applied documents by Fink, Joyce, Baum, and Lyle as the combination of the applied documents by Fink, Joyce, and Baum has already addressed the argued claim feature of independent claims 1 and 50 according to the rationale stated above. In addition, each of the features of the dependent claims 6 and 54 is rendered obvious based on the combination of the applied documents by Fink, Joyce, Baum, and Lyle.

(10) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Shaw, Yin-Chen

/Yin-Chen Shaw/

Dec. 14, 2010

Conferees:

LaForgia, Christian

/Christian LaForgia/

Primary Examiner, Art Unit 2439

Orgad, Edan

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439